(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2003 (05.06.2003)

PCT

(10) International Publication Number
WO 03/046748 A1

(51) International Patent Classification[7]: G06F 15/16

(21) International Application Number: PCT/US02/38231

(22) International Filing Date:
27 November 2002 (27.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/334,312 28 November 2001 (28.11.2001) US
60/334,162 28 November 2001 (28.11.2001) US

(71) Applicant: **VISIONSHARE, INC.** [US/US]; 2550 University Avenue West, Suite 310 South, St. Paul, MN 55114 (US).

(72) Inventors: **FRASER, John, D.**; 401 Westwood Drive South, Golden Valley, MN 55416 (US). **PALMER, Peter, L.**; 2302 Brewster Street, St. Paul, MN 55108 (US). **HALLGREN, Jeffry, H.**; 355 Highway 7, Excelsior, MN 55331 (US).

(74) Agent: **SIEFFERT, Kent, J.**; Shumaker & Sieffert, P.A., Suite 105, 8425 Seasons Parkway, St. Paul, MN 55125 (US).

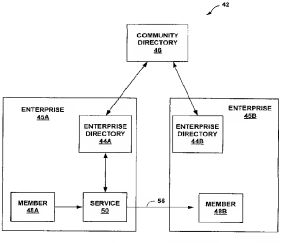
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: DIRECTORY-BASED SECURE NETWORK COMMUNITIES USING BRIDGING SERVICES



(57) Abstract: Techniques are described for constructing and maintaining secure communities over a computer network, such as the Internet. In particular, the techniques allow security to be integrated and managed in a "directory-centric" fashion. In other words, the techniques described herein allow a community of trusted members (48A, 48B) to easily be managed via one or more online directories (46) rather than hierarchical certification authorities. In addition, the invention provides techniques for validating security credentials locally within an enterprise (45A, 45B). A trust server within the enterprise (45A, 45B) intercepts a validation request from a secure electronic service (50) within the enterprise. If the trust server is unable to answer the validation request, the trust server queries a bridge service provider, which associates the trust server with trust servers maintained by other enterprises. for the security credential information necessary for validation.

WO 03/046748 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

DIRECTORY-BASED SECURE NETWORK COMMUNITIES USING BRIDGING SERVICES

TECHNICAL FIELD

[0001] The invention relates to computer networks and, more particularly, to secure information exchange and other operations via computer networks.

BACKGROUND

[0002] Whether fearful of email eavesdropping, being hacked in corporate networks or accidentally losing important information, many companies and government organizations continue to invest huge sums of money on private networks, virtual private networks (VPNs), dialup modem banks, and similar technologies, to sidestep or ameliorate problems associated with Internet usage. Nevertheless, broad corporate acceptance of network-based communications and other operations involving sensitive information has been slow due to the lack of a comprehensive security system that provides end-to-end trust and reliability for important business information flows.

[0003] Often, an organization may resort to a wide variety of conventional techniques involving a collection of disparate technologies in an attempt to address these concerns. Many organizations, for example, rely extensively on the use of basic of security information, e.g., usernames and passwords, and may issue such information to virtually all members, whether employed or contracted. Many of these organizations use symmetric key cryptographic technologies, such as *Pretty Good Protection* (PGP), to encrypt files or documents for transfer over the Internet, relying on telephone calls or other out-of-band methods to exchange the electronic keys used to lock and unlocks these files. Others are beginning to use S/MIME to encrypt and sign emails between "islands" of trading partners. Still others are leasing "private" communication lines believing that these lines reduce the need for encryption of information. The use of the wide variety of conventional techniques leads to a lack of integration and scalability. Enterprises that use different Certificate Authorities, for example, may not be able to securely

communicate with one another since each enterprise uses a different type of digital certificate.

SUMMARY

[0004] In general, the invention is directed to techniques for constructing and maintaining secure communities over a computer network, such as the Internet. In particular, the techniques allow security to be integrated and managed in a "directory-centric" fashion. In other words, the techniques described herein allow a community of trusted members to easily be managed via one or more online directories rather than hierarchical certification authorities. The techniques described herein further allow validation of security credentials locally within an enterprise via a bridging service

[0005] The term "community" is used to refer to a collection of trusted members that securely interact via one or more networks in accordance with the techniques described herein. Further, the members may belong to one or more member enterprises. For example, a medical institution, such as a hospital, clinic, or medical research facility, may employ the techniques described herein to maintain a secure network community for employees or other individuals associated with the medical institution. In addition, that medical institution may belong to a higher-level network community along with a number of other medical institutions.

[0006] The directories managed by a community provides the identity and management information needed to support advanced electronic communications features. Moreover, the "trust" associated with an identity of a network user can be locally managed primarily by controlling a membership of that user in the directory. The underlying security technologies, such as digital certificates, are seamlessly utilized by the directory-based techniques to enforce and facilitate that trust. In this manner, the directory-oriented techniques can be used to build and maintain trusted communities using policies, member directories and related technologies to supply the security needs within these communities.

[0007] Further the techniques allow for validation of security credentials, also referred to as authentication, across multiple enterprises via a bridging service. A trust server maintained locally within an enterprise may validate security

credentials for clients within the enterprise by accessing security credential information of other trust servers via the bridging service. The term "trust server" is used to refer to a server that participates in validation of security credentials via the bridging service.

[0008] The trust server may, for example, intercept a validation request from an electronic service being used by a client. The electronic service may include, for example, a secure electronic email service. The trust server accesses security credential information, which may be stored in a directory, for example, to determine an answer for the validation request. The directory may include information, such as a digital certificate, contact information, an email address, and other information that uniquely identifies the respective client.

[0009] If the trust server is unable to answer the validation request, the trust server queries a bridge service provider external to the enterprise for the security credential information necessary for validation. The bridge service provider associates the trust server with trust servers maintained by other enterprises, and forwards the query to the appropriate one of the trust servers maintained by the other enterprises. The trust server of the other enterprise returns the necessary security credential information, which the bridge service provider relays to the querying trust server for validation. Alternatively, the bridge service provider may answer the query on behalf of enterprises that are clients of the bridge service provider. For example, the bridge service provider may maintain a directory of security credential information of enterprises that are members and access that directory to search for the appropriate security credential information. In this manner, validation (or authentication) is performed locally within enterprises.

[0010] In one embodiment, the invention is directed to a system comprising a server having a directory of members of a network community, wherein the directory stores data defining digital identities of the members for securely exchanging information with the members. A software application executing on a network device coupled to the server accesses the directory and exchanges the information between the members in accordance with the digital identities of the members.

[0011] In another embodiment, the invention is directed to a system comprising a community directory of members of a network community, wherein the members are associated with a plurality of enterprises, and a plurality of enterprise directories linked to the community directory, wherein the enterprise directories stored data defining digital identities for subsets of the members associated with the enterprises. The system further comprises a software application operating within a first one of the enterprises for exchanging information between the members of the community, wherein the software application accesses the enterprise directory associated with the first enterprise to securely exchange the information in accordance with the digital identities of the members.

[0012] In another embodiment, a method comprises receiving a request for exchanging information with a member of a network community, and accessing a directory to retrieve a digital identity for the member. The method further comprises applying the digital identity to the information to produce a secure communication, and sending the secure communication to the member.

[0013] In one embodiment, the invention provides a system comprising a client service executing within an enterprise and a trust server to receive validation requests from the client service and perform security credential validation within the enterprise.

[0014] In another embodiment, the invention provides a method comprising receiving a validation request from a client service within an enterprise and performing security credential validation within the enterprise using a trust server.

[0015] The invention may provide one or more advantages. For example, unlike conventional directory-management tools, such as Lightweight Directory Access Protocol (LDAP) tools, the techniques allow seamless management of digital certificates or other security or cryptographic mechanisms using directory-oriented mechanisms. As a result, digital certificate or other security mechanisms become "attributes" of a member to form his or her "identity" within the directory. As a result, a directory may be viewed as containing a superset of identities for members, such as an email address and similar information, necessary to support the network services required by the community.

[0016] Consequently, the trust established between the members lies primarily with membership in the directory and the method used to mange these members. This trust, therefore, need not rely exclusively on external parties, such as a certificate authority that issues the digital certificates used by the members of the community. As a result, the established trust between members flows primarily from the directory and its management, and not from a certificate authority (CA) or other party external to the community. Unlike a hierarchy of certificate authorities, the directory-based techniques described herein provide the "trust" for founding a secure network community to be distributed and managed locally by the members of the community. In this manner, the techniques may be viewed as shifting the ultimate control and focus of network trust inward to communities of members from these external parties, as is typically required by conventional security mechanisms.

[0017] Further the bridge providers may allow enterprises to obtain validation security locally without cooperation between the enterprises to establish common security models. For example, the trust servers may provide validation of security credentials without exchanging public-private key pairs, cooperating on setting up private lines, or agreeing to a specific Public Key Infrastructure (PKI) implementation. In this manner, bridge providers may interconnect enterprises using different security environments allowing for a high degree of scalability. Further, the bridge service providers provide that ability to use multiple types of digital certificates from various Certification Authorities.

[0018] The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF DRAWINGS

[0019] FIG. 1 is a block diagram illustrating a system that utilizes directory-based techniques to construct and manage use of a secure network community.

[0020] FIG. 2 illustrates an example embodiment of a directory for providing secure network communities in accordance with the techniques of the invention.

[0021] FIG. 3 illustrates an example embodiment of a member object of an online directory for establishing a secure network community.

[0022] FIG. 4 is a block diagram that illustrates the function of the directory of FIG. 2 when operating as an enforcement agent to ensure that electronic inter-client interactions within a community conform to member-approved policies.

[0023] FIG. 5 is a block diagram in which a plurality of enterprise directories are chained to a higher-level trusted community directory associated with a common community.

[0024] FIG. 6 is a block diagram illustrating the management of online directories by registration agents (RA).

[0025] FIG. 7 is a block diagram illustrating a system in which a secure message center makes use of the techniques described herein.

[0026] FIG. 8 is a block diagram of an example system that illustrates use of the techniques to allow firewalls, network servers, routers, or other network devices to authenticate community members.

[0027] FIG. 9 is a block diagram of a system in which a community is interconnected with one or more other communities via open bridge services.

[0028] FIG. 10 illustrates an example interface with which one or more registration agents interact to manage the digital identifies and security mechanisms associated with directory-based secure communities.

[0029] FIG. 11 illustrates an example interface presented by the directory management module when the registration agent elects to view or modify the digital identity of the member.

[0030] FIG. 12 illustrates and exemplary view of various details for a certificate associated with a member.

[0031] FIG. 13 is a block diagram illustrating a trust domain that provides substantially instant validation of security credentials across multiple enterprises.

[0032] FIG. 14 is a block diagram illustrating a trust domain in further detail.

[0033] FIG. 15 is a block diagram illustrating a trust server that validates security credentials locally within an enterprise.

[0034] FIG. 16 is a block diagram illustrating a bridge service provider that links trust servers together to form a trust domain, such as trust domain of FIG. 13.

[0035] FIG. 17 is a flow diagram illustrating instant validation of security credential information locally within an enterprise.

DETAILED DESCRIPTION

[0036] FIG. 1 is a block diagram illustrating a system 2 that utilizes the directory-based techniques described herein to construct and manage use of a secure network community 4. As illustrated, community 4 includes an on-line community directory 6 that supports the identification, management and usage of the digital identities of members 7A-7N ("members 7").

[0037] Moreover, community directory 6 seamlessly integrates security technologies to support the secure interaction 8 of members 7. For example, members 7 may utilize community directory 6 in accordance with the techniques described herein to securely exchange electronic mail messages or files, effect secure network-based transactions, and the like.

[0038] In addition, community directory 6 acts as an enforcement agent to ensure that electronic inter-client interactions 8 within community 4 conform to member-approved policies defined by policy information 9. Specifically, community directory 6 maintains policy information 9 to control policy enforcement via an online directory. Specifically, members 7 of community 4 agree to a standard policy to control membership.

[0039] For example, policy information 9 may include data that defines how new members are added or removed from directory 6, and the general usage and security of the directory infrastructure, as described herein. In accordance with policy information, for example, community directory 6 may issue digital certificates to any new members as part of the registration and enrollment process. Policy information 9 may further require that removable media must be used between any server issuing the certificates and the network-based community. In other words, policy information 9 may require an "air gap" between the issuing server and the network as an extra layer of security to ensure the confidentiality of any digital identity of a member is not compromised.

[0040] FIG. 2 illustrates an example embodiment of a directory 20 for providing secure network communities in accordance with the techniques described herein. As illustrated, directory **20** defines one or more member objects 22. Each member object 22 supports the ability to invoke specified security mechanisms, e.g., digital certificates, keys and other identifiers, for secure network-based exchanges of information.

[0041] Member objects 22 are addressable to locate specific information for community members, and allows electronic services provided within the community, e.g., a mail service, to easily invoke the relevant electronic security messages to securely exchange information. For example, the mail service may access one or more of member objects 22 to digitally sign and encrypt electronic documents for exchange between the members of the community.

[0042] FIG. 3 illustrates an example embodiment of a member object 24 of an online directory for establishing a secure network community. In this example embodiment, member object 24 may conform to the Lightweight Directory Access Protocol (LDAP), and may use the *inetOrgPerson* object class and other object classes defined by the protocol for storing information to formulate the identity of the members. For example, member object 24 includes a member schema 26 that defines the *inetOrgPerson* schema, an X.509 or other digital certificate 27, a PGP schema 28, an email address 29, and other information that uniquely identifies the respective member, such as an electronic photograph, retinal scan, fingerprint scan, and the like. Other object classes may be stored within directory 22 and used by the community, e.g., server objects, security objects, firewall objects, and the like.

[0043] FIG. 4 is a block diagram that illustrates the function of directory 38 when operating as an enforcement agent to ensure that electronic inter-client interactions within a community conform to member-approved policies. Initially, an originating member 30A initiates an exchange of information with member 30B by invoking electronic service 34. Electronic service 34 may be any of a variety of network-based services for securely exchanging information, such as electronic mail, electronic file sharing, network storage, secure web folders, secure web access, and the like.

[0044] In response, electronic service 34 queries or otherwise accesses online directory 38 to retrieve all necessary identity information and invoke the necessary security mechanisms required by the community for communicating with member 30B. Consequently, the electronic service 34 may access directory 38 to automatically validate and return any public digital certificate or other digital credential for member 30B. Upon receiving the digital credential and validation from directory 38, service 34 formulates and sends the electronic communication 39 to member 30B.

[0045] Upon receipt, member 30B queries directory 38 for confirmation of the digital identity associated with the received communication 39, i.e., the identity of member 30A. For example, member 30B may access directory 38 to retrieve a public key associated with member 30A for verification that communication 39 was indeed sent by member 30A. This directory-based security authentication process may occur in real-time, and may ensure, for example, that a digital certificate or other credential is valid, the certificate has not been revoked, and that the owner of the certificate is a current member of community, i.e., a member listed within directory 38. In this manner, directory 38 enforces compliance with member-approved, directory-maintained policies and security mechanisms.

[0046] FIG. 5 is a block diagram in which a plurality of enterprise directories 44 are chained to a higher-level trusted community directory 46 associated with a common community. Enterprise directories 44 correspond to separate enterprises 45A, 45B, and may provide directory-based security for the members of the enterprises, e.g., member 48A and member 48B. In this manner, enterprise directories 44A may be linked to one or more higher-level directories, e.g., community directory 46 for managing and enforcing policies for secure information exchange within the community. Enterprises 45 may be any organization or institution. For example, a number of medical organizations, hospitals, clinics, medical research facilities, and the like, may utilize the techniques to construct and manage a secure network-based community in which information exchanges within the community comply with agreed-upon policies.

[0047] Enterprise directories 44 may be linked to the trusted community directory 46 via any of a number of techniques, including replication of all or portions of the

data stored within member directory 46, chaining to another directory, or by making referrals to another directory that is authorized to serve specified account details.

[0048] As illustrated in FIG. 5, an originating member 48A of enterprise 45A initiates a secure exchange of information with member 30B of enterprise 45B. Specifically, member 48A invoking electronic service 50 supported by the first enterprise. For example, electronic service 50 may be an electronic mail service, a file exchange service, a messaging service, and the like.

[0049] In response, electronic service 50 queries or otherwise accesses enterprise directory 44A to retrieve all necessary identity information and invoke the necessary security mechanisms required by the community for communicating with other members of the community, e.g., member 48B.

[0050] If enterprise directory 44A does not contain the necessary identity information for the requested member, i.e., member 48B, then the directory will in turn query community directory 46. If community directory 46 is able to service the request, the community directory 46 may respond directly to enterprise directory 44A. Otherwise, community directory 46 will query enterprise directory 44B of enterprise 45B to obtain the necessary identity information associated with member 48B. For example, community directory may query the enterprise directory 44B for validation of a public certificate of member 48B, and returns the public certificate or other digital credential to service 50. Upon receiving the digital credential and validation from community directory 46, service 50 formulates and sends the electronic communication 56 to member 48B of the second enterprise.

[0051] Upon receipt, member 48B queries enterprise directory 44B for confirmation of the digital identity associated with the received communication 50, i.e., the identity of member 48A. Enterprise directory 44B may query community directory 46, which may in turn query enterprise directory 44A to confirm the digital identity of member 48A. Community directory 46 may, for example, retrieve from enterprise directory 44A a public key associated with member 48A, verification that communication 56 was indeed sent by member 48A.

[0052] In this manner, the techniques described herein allow enterprises 45 to maintain their own directories for their respective members. Further, each enterprise directory 44 need not supply all information regarding the members of enterprises 45 to community directory 46. In particular, enterprise directories 44 need only supply community directory 46 with the information necessary to securely communicate with those specific individuals within enterprises 45 who need to be members of community directory 46.

[0053] Management of community directory 46 is performed by one or more registration agents (RAs) 58 associated with enterprises 45.

[0054] FIG. 6 is a block diagram illustrating the management of online directories by registration agents (RA). As illustrated, RA 60 manages community directory 62 via directory management module 64. RA 60 is an individual charged and contractually obligated to get and maintain accurate identity information for members associated with the network community. For example, RA 60 may request and approve digital certificates for addition to the member objects of community directory 62.

[0055] A network community may further include a community-level registration agent, i.e., RA 66 that interacts with directory management module 68 to manage the identity information for members 70 stored within enterprise directory 72 of enterprise 74. Alternatively, this information may be received from lower-level enterprise directories, e.g., enterprise directory 72.

[0056] In one embodiment, management modules 64, 68 provide graphical user interfaces to manage the digital identifies and security mechanisms associated with directories 62, 72, respectively. Moreover, management modules 64, 68 may integrate directory management, certificate management and other administrative tasks via a simple directory-oriented approach. Modules 64, 68 may provide, for example, all of the functionality needed to enroll a member, request a certificate for that member, and install the certificate within the appropriate directory 62, 72. Modules 64, 68 also provides for querying and management of members once they have been added to directories 62, 72. Moreover, modules 64, 68 support fine-grained access control so that read accesses and modifications to members of the

respective directories 62, 72 are controlled at the member level using certificate access control which enforces the delegation of administrative privileges.

[0057] Policy information 78 includes specifications and particular policies to control the process by which RAs 60, 66 manage directories 62, 72. In this manner, consistent policies for management of members may be defined and applied to all directories within a network community, e.g., directories 62, 72. As an example, one configuration of policy information 78 may define the following requirements: (1) community directory 62 shall be compliant with the Lightweight Directory Access Protocol (LDAP), (2) only authorized RAs 60, 66 can add, remove, or otherwise modify the digital identifies of members of the respective directories 62, 72, (3) RAs 60, 66 will be the first users added to community directory 62, and all information related to their role must be included in the community directory, such as a color photograph that is less than 5 years old, (4) each of RAs 60, 66 must be a notary public in good standing in the state in which he or she reside, (5) RAs 60, 66 may only interact with community directory 62 according to the community approved policies and tools, and (6) each of RAs 60, 66 must check the identity of members of the respective directories 62, 72 using agreed-upon policies, and they must meet with members 48 in-person to verify policy-approved identifications.

[0058] In this fashion, directories 62, 72 can seamlessly integrate community-wide policies and security mechanisms with network services provided by the community, e.g., services 80 provided by enterprise 74. One example of electronic services 80 includes a secure electronic mail service. These techniques allow, for example, members 70 and service 80 to first identify other members within the community via their role within the community, and then automatically access their digital identity and other security information necessary to exchange secure email with the members.

[0059] As another example, services 80 may utilize the techniques to provide secure file transfer between members 70. Services 80 may provide a seamless end-to-end communication of files between members by a "drag-and-drop" interface on a desktop of one of the members, e.g., one of members 70 within enterprise 74. In

response, services 80 may verify the signature of the sending member 70 against the enterprise directory 72.

[0060] As another example, services 80 may utilize these techniques to provide secure access to information stored within the community. Consequently, members within the community, e.g., members 70 within enterprise 74, may be able access to a number of resources by having their digital identity included in the directory, which allows network servers within the community to easily verify their identities, and thereby support a fine-grain access control mechanism. As one example, web or storage servers within the community may be linked to the community directories, e.g., community directory 62 and enterprise directory 72. As a result, each secure server within a community, for example, need not build separate lists of trusted members, including and all their attributes. Instead, these servers need only maintain lists of links to member objects within one or more of directories 62, 72. This allows the servers to query directories 62, 72 in response to an access request for immediate determination of whether the accessing party is still a member of the community in good standing, and whether he or she has permission to access the particular requested resource. In addition, as required by policy information 78, registration agents 60, 66 may automatically allocate storage space within one or more of the servers and provide access to community files adding a new member to the community. For example, upon adding a new member to enterprise 74, enterprise directory 72 may issue a single certificate as part of the digital identify of the new member, and that certificate may provide access to multiple objects within the community, including objects within other enterprises.

[0061] As another example, services 80 may utilize the directory-driven techniques described herein for secure message exchanges using digitally-signed documents. In other words, community members 70 can easily digitally sign documents using the certificates stored in the directories 62, 72. Similarly, recipients of these documents are able to verify the digital signatures via certificates stored within community directories 62, 72 to increase the trust of these signatures. This may be advantageous in enabling a truly paperless network

community for conventional paper-based processes that required hand-written signatures.

[0062] To aid in the seamless validation and authentication of electronic communication between members 70, an enterprise mail server within enterprise 74 may process non-member mail in normal fashion, but may automatically redirect electronic mail for community members to a second server configured to authenticate the members within the community. A member authentication service executing on this server, may receive the redirected electronic mail, and provide functionality for digitally signing and verifying of the email between the members in accordance with the directory-based techniques describe herein. Specifically, the member authentication service may access directories, 72, 62 to retrieve and validate certificates or keys associated with the members to enforce secure email exchange. This may allow for the immediate creation of a community secure email infrastructure by allowing the email systems within the community to verify digital signatures and identities via the directories, e.g., enterprise directory 72 and community directory 62.

[0063] FIG. 7 is a block diagram illustrating a system 90 in which a secure message center 92 makes use of the techniques described herein. In the example system 90, message center 92 provides seamless integration of web-based email with other protocols for communicating network messages.

[0064] Initially, a patient 94 initiates a communication 102 using one or more web-based forms presented by message center 92. Patient 94 may not provide a digital certificate with communication 102, however, a web server or other application server within message center 92 digitally signs communication 102 on behalf of patient 94. In addition, another community member, such as doctor 96, initiates communication 104 that may utilize a different communication protocol, such as a standard email software application using the S/MIME protocol. Specifically, doctor 96 may initiate communication 104 via a secure electronic email service mechanism for exchanging information with patient 94

[0065] In accordance with the techniques described herein, message center 92 accesses community directory 98, and possibly one or more enterprise directories 100, to validate the signature provided on behalf of patient 94, as well as the

signature provided by doctor 96. In other words, message center 92 may access directories 98, 100 to confirm identities of both parties. In this manner, message center 92 is able to provide for the "ad-hoc," web-based message exchange directly between two or more members of the community in a secure manner without pre-configuring or pre-establishing any communication, security information, or trust paths between the members.

[0066] FIG. 8 is a block diagram of an example system 110 that illustrates use of the techniques to allow firewalls, network servers, routers, or other network devices to authenticate community members. Initially, a community member, e.g., member 120 of enterprise 112B initiates a communication 122 that consumes, accesses, or otherwise communicates with a network device, e.g., firewall 124 of enterprise 112A.

[0067] In response, firewall 124 of enterprise 112A queries enterprise directory 116A, which may trigger accesses to community directory 118 and enterprise directory 116B associated with member 120 as described above, to determine whether the requested service should be permitted. If the requested service is permitted, firewall 124 may forward the request to another network device, e.g., router 126.

[0068] In similar fashion, router 126 accesses enterprise directory 116A to verify other digital identity information, such as an Internet Protocol (IP) addresses for the sender or other packet-level information. The verification may trigger additional requests to community directory 118 and enterprise directory 116B for validation of the information based on the digital identify for member 120. If the information is validated, router 126 may permit communication 122 to access one or more of services 128 offered by enterprise 112A.

[0069] Services 128 may additionally validate other information associated with the identity of member 120 in similar fashion. If this validation is successful, services 128 may provide the network service requested by member 120, such as communication of an electronic mail message to another member, secure access of a file or other network object, and the like. Consequently, the directory-based techniques described herein can be used to readily handle and facilitate multiple

layers of security via various network devices or services within an enterprise in a manner that applies community-approved security policies at each level.

[0070] FIG. 9 is a block diagram of a system 130 in which a community 134 is interconnected with one or more other communities 138 via open bridge services 136. In general, this interconnection enables these trusted communities 134, 138 to easily expand their trust domain beyond the members of any individual community to other directory-based secure communities.

[0071] More specifically, enterprise directories 140 of community 134 may lack necessary information to answer a request for identity information, and may in turn access community directory 142, as described in detail herein. If community directory 142 is also unable to provide the requested information, community directory 142 initiates a query to open bridge services 136. Open bridge services 136 is responsible for, and contractually bound to, forward these queries to the most appropriate community directory 138 for services the request. As one example, the open bridge services 136 may forward the request to the Federal E-Authentication Service, or other communities located in other states or even other counties.

[0072] FIG. 10 illustrates an example interface 150 with which one or more registration agents interact to manage the digital identifies and security mechanisms associated with directory-based secure communities. Directory management module 64 of FIG. 5, for example, may present interface 150 to registration agent 50 as a graphical user interface (GUI) for managing community directory 62.

[0073] The illustrated example interface 150 includes a first input area 152 from which a registration agent may invoke a number of tasks for managing the directory. For example, the registration agent may search for a specific member within the directory, add or import new member certificates, track the status of pending certificate requests, import certification revocation lists (CRLs), and other operations.

[0074] If the registration agent invokes a find user operation via first input area 152, for example, interface 150 present a search area 158 that allows the registration authority to search by a variety of options, including full name,

employer, last name, phone number, work unit, email, and the like. Based on the provided search criteria, the directory management module presents interface 150 to include a list 160 of matching members. The registration agent may select one or more of the members to update his or her identity information, or remove the member from the community.

[0075] In this manner, interface 150 provides an integrated graphical environment for accessing and managing the digital identities associated with members of the community. In response to input received from a registration agent via interface 15, the directory management module accesses the member objects of the directory, e.g., member objects 22 of FIG. 2, to locate, modify, or otherwise update specific identity information for community members. By interacting with interface 150, the registration agents can easily manage the directory information, policy information and security mechanisms for the community

[0076] FIG. 11 illustrates an example interface 162 presented by the directory management module when the registration agent elects to view or modify the digital identity of the member. As illustrated, interface 162 presents a variety of identity information as retrieved from the directory being managed. For example, interface 162 may present the organization, phone, email address, physical address, a photograph, and the like, as shown by 164 and 166. In addition, interface 162 presents security information, such as the date the member was registered with the community and issued a digital certificate, a certificate valid unit, and the registration agent that added the member and verified his or her information.

[0077] In addition, interface 162 includes selection mechanism 168 with which the registration agent can view various details for the certificate associated with the member and stored within the directory, as presented by interface 170 of FIG. 12. In this manner, interface 170 allows a registration agent to view and manage the details of the security mechanisms for the community, e.g., digital certificates, and the like, as stored and maintained within a community or enterprise directory.

[0078] FIG. 13 is a block diagram illustrating a trust domain 210 that provides substantially instant validation of security credentials across multiple enterprises 212A-212E ("212"). More particularly, enterprises 212 include trust servers 214A-214E ("214"), respectively, which validate security credentials for clients

within trust domain 210. The term "trust server" is used to refer to a server that participates in validation of security credentials within trust domain 210.

[0079] Each of enterprises 212 and, more particularly trust servers 214 associated with enterprises 212, are coupled to at least one of bridge service providers 216A-216N ("216"). Bridge service providers 216 serve to link trust servers 214 of enterprises 212 together, in turn creating trust domain 210. When a service provided to a client of an enterprise 212 requires validation of security credential information that is maintained by a trust server 214 within another one of enterprises 212, for example, one or more bridge service providers 216 provide the link through which the client obtains security credential information.

[0080] Trust domain 210 allows clients within one of enterprises 212 to obtain validation of security credentials, e.g., without cooperation between enterprises 212 to establish a common security model. For instance, enterprises 212 may provide security credential validation without exchanging public-private key pairs, cooperating to set up private lines, or agreeing to a specific Public Key Infrastructure (PKI) implementation. In this manner, bridge service providers 216 may interconnect enterprises 212 using different security models. The interconnection of enterprises 212 using different security models may provide the ability to use multiple types of digital certificates as well as check digital certificates from various Certification Authorities. For example, trust domain 210 may be configured to support X.509 certificates, along with other types of certificates or new technologies by using eXtensive Markup Language (XML) to define Standard Object Access Protocol (SOAP) calls. For instance, SOAP calls may be used to validate X.509 certificates, Pretty Good Privacy (PGP) keys, Kerberos keys, or to find a digital certificate of a client. Bridge service providers 216 allows for a high degree of scalability by reducing the number of direct interconnections needed for secure communication between enterprises 212.

[0081] As mentioned above, trust servers 214 may validate security credentials within trust domain 210. For example, trust server 214A within enterprises 212A may validate security credentials for clients within enterprises 212A. Trust servers may further provide security credentials for use in validation performed by other trust servers 214. For example, trust server 214A may provide security credentials

to trust server 214B through bridge service providers 216 for use in validation for a service within enterprise 214B. Although in FIG. 13 each of enterprises 212 includes a single trust server 214, enterprises 212 may include more than one trust server 214 to provide redundancy and ensure reliability.

[0082] More specifically, one of trust servers 214, such as trust server 214A, receives a validation request from a service being used by a client. Trust server 214A, for example, may be configured to intercept a validation request, which is usually sent to a third party for validation processing, of a client within enterprise 214A and answers the validation request locally within enterprise 212. Trust server 214A may, for example, be linked to or be a part of a certificate authority system within enterprise 212A and answer the validation request using a local certificate revocation list (CRL) or an online certificate status protocol (OCSP) responder. Alternatively, trust server 214A may be loaded with the security credential information in a directory, such as a cache, or other storage mechanism.

[0083] When trust server 214A is unable to answer the validation request, trust server 214A forwards a query for the security credential information necessary for validation to bridge service provider 216 associated with the respective trust server 214. Bridge service provider 216 associated with the respective trust server 214 may answer the query on behalf of another enterprise 212. Bridge service providers 216 that are not able or not authorized to answer the query on behalf of the other enterprise 212 forward the query for the security credential information to another bridge service provider 216 or trust server 214 that can obtain the security credential information. Bridge service providers 216 forward the query by accessing a trust server 214 associated with another one of enterprises 212 and obtaining the necessary security credential information from trust server 214 associated with the other enterprise 212. Bridge service providers 216 relay the security credential information to trust server 214A associated with the client that made the validation request.

[0084] The security credentials may be a digital certificate or a technology like biometrics that uniquely binds a digital identity to an individual client. The security credential information that bridge service providers 216 relay to trust server 214A may include, for example, validity dates of the digital certificate, the

status of the digital certificate, i.e., active or revoked, XML-structured contact information for the client associated with the digital certificate, and the like. The communications between the clients, trust servers 214, and bridge service providers 216 can be, for example, a series of simple object access protocol (SOAP) calls. Trust server 214 associated with the client receives the security credential information, parse the security credential information, and processes the security credential information to control the service being used. For instance, trust server 214 may allow the client to send a secure email when the security credentials are validated with the obtained security credential information or prevent the client from sending the email when the security credentials are not validated.

[0085] A single source of authentication may not be preferred from a privacy perspective. Initial identity may be provided to clients that act in an enterprise-to-enterprise role, and not for individual clients. Most clients, for example, are comfortable with a publicly known enterprise identity, especially one that does not contain any personal information about the client. Example usages of this type of trust domain for validation of security credentials include ordering products for enterprises 212, signing an electronic contracts, purchasing with a credit card, ordering products over the web, sending medical records between providers, withdrawing money from your local ATM system, voting, betting, getting licenses from various local, state and federal agencies, proving age when buying liquor, paying parking meters, paying for pay-telephone calls, paying for public transportation, and the like.

[0086] Enterprises 212 within trust domain 210 may, however, require a stricter security model for validation of security credentials. Some examples of trust domains that may require stricter security models include a health care insurance company that accepts claims signed only by certificates issued under specific policies, a pharmacy chain that accepts electronic prescriptions that comply with a Pharmacy Association policy, state government agencies allow people to vote with certificates that fall within a group of specific policies and are verifiable at point of voting, and organizations that accept purchase orders above a certain dollar amount only if digitally signed.

[0087] Trust domain 210 may be created, for example, by contractual arrangements between enterprises 212 and bridge service providers 216. Multiple vendors may provide the bridging service, using standards that are agreed to by enterprises 212. Further, the standards under which the bridging services operate may provide for national and perhaps international interoperability. The vendors providing the bridging services may be contractually bound to operate in a professional manner and may further be required to upgrade the bridging systems as new features are added. The vendors providing the bridging services may further be audited on a regular basis. The regulations imposed on the vendors providing the bridging services, along with the contracts entered by the vendors, instill a sense of trust in the bridging vendors.

[0088] FIG. 14 is a block diagram illustrating another example trust domain 218 that provides substantially instant validation of security credentials across multiple enterprises in further detail. Trust domain 218 includes enterprises 212A and 212B ("212"). Each of enterprises 212 includes a corresponding plurality of trust servers 214. In the example of FIG. 13, enterprise 212A includes trust servers 214A-214K and enterprise 212B includes trust servers 214A-214M.

[0089] Each of trust servers 214 of enterprises 212 corresponds to one or more bridge service providers 216A-216N ("216"). Trust servers 214 of enterprise 212A may, for example, correspond to bridge service provider 216A while trust servers 214 of enterprise 212B correspond to bridge service provider 216N. Alternatively, trust servers 214 of enterprise 212A may correspond the same bridge service provider 216 as trust servers 214 of enterprise 212B. However, all of trust servers 214 within each of enterprises 212 must not correspond to the same bridge service provider 216. For example, a portion of trust servers 214 of enterprise 212A may correspond to bridge service provider 216A while the rest of trust servers 214 of enterprise 212A correspond to bridge service provider 216N.

[0090] Trust servers 214 communicate with corresponding bridge service providers 216 in order to validate security credentials for clients. Bridge service providers 216 may further communicate with each other in order to identify security credential information necessary for validation. For example, bridge

service providers 216 may communicate when trust servers 214 associated with the sender and receiver correspond to different bridge service providers 216.

[0091] As described above, the trust domains may support many client services. One such client service supported by trust domain 218, which is described for purposes of illustration, is secure email services. Other client services include electronic file sharing, network storage, secure web folders, secure web access, and the like. Clients 220 within enterprises 212 can use the infrastructure of trust domain 218 to lookup other clients, find digital certificates associated with the other clients, and email the clients with secure multipurpose internet mail extensions (S/MIME) emails. At the receiving end, the receiving client can validate included digital signatures using the same mechanism.

[0092] For example, a client 220A of enterprise 212A starts a communication process by accessing a desired service locally. The communication process may include electronic mail (email), document signing, transferring files, or the like. For example, client 220A of enterprise 212A may wish to send a secure email to client 220B of enterprise 212B and, in turn, accesses a local secure email service. The local secure email service may, for example, be a software program on a device operated by user 220A. Before the secure email service sends the email, the email service queries a validation request, such as a request for validation of active digital certificates associated with the source client 220A and destination client 220B. One of trust servers 214 of enterprise 220A intercepts the request for validation of security credentials.

[0093] Trust server 214 that intercepted the validation request accesses stored security credential information to determine whether an answer to the validation request may be granted. Trust server 214 may, for example, be linked to or be a part of a certificate authority system within enterprise 212A and answer the validation request using a local certificate revocation list (CRL) or an online certificate status protocol (OCSP) responder. Alternatively, trust server 214A may be loaded with the security credential information in a cache or other storage mechanism. Trust server 214 may, for example, access the cache of security credentials maintained within enterprise 212A.

[0094] When the intercepting trust server 214 cannot grant the validation request, trust server 214 may query a corresponding bridge service provider 216 in order to retrieve the necessary security credential information to grant the validation. Bridge service provider 216 obtains the security credential information necessary for validation of the security credentials by the intercepting trust server 214. Each of bridge service providers 216 may maintain a directory of members of bridge service provider 216. The directory may include, for example, a unique identifier, a certificate number, and a reference for security credential information location for each of the members. The reference for security credential information may, for instance, be a lightweight directory access protocol (LDAP) directory. Alternatively, bridge service providers 216 may answer the queries on behalf of their clients by running local trust servers. The functionality of the trust server run by bridge service providers 216 is the same as trust servers 214 of enterprises 212. For example, if trust servers 214 of enterprises 212 correspond to the same bridge service provider 216, bridge service provider 216 may maintain have the necessary security credential information.

[0095] If bridge service provider 216 corresponding to the intercepting trust server 214 does not have the necessary security credential information and trust servers 214 of enterprises 212 correspond to the same bridge service provider 216, bridge service provider 216 may query the trust server 214 of enterprise 212B to obtain the necessary security credential information. If trust servers 214 of enterprises 212 correspond to different bridge service providers 216, bridge service provider 216 associated with enterprise 212A may query another bridge service provider 216 associated with enterprise 212B to obtain the security credential information.

[0096] Upon receiving the security credential information, intercepting trust server 214 associated with client 220A parses the security credential information and processes the security credential information to control the communication process being used by client 220A. For instance, intercepting trust server 214 may allow the client to send a secure email when the security credentials are validated with the obtained security credential information or prevent the client from sending the email when the security credentials are not validated. Upon validating the security credentials trust server 214 logs the validation to provide an audit trail.

[0097] A similar process occurs on the receiving end of the communication process. More particularly, client 220B receives the communication, e.g., a secure email. Client 220B accesses the email service to open the email. Before opening the email, the email service queries a validation request that is intercepted by a corresponding trust server 214 of enterprise 212B. Trust server 214 obtains security credential information from within trust server 214 itself or via bridge service provider 216. Trust server 214 associated with client 220B parses the security credential information and processes the security credential information to control the process being used by client 220B.

[0098] The techniques described above for secure email services may be extended to a number of different client services. The clients can be any type of system. The client could be a door that checks the validity of a wireless digital certificate in order to determine whether to unlock or remain locked. The client could also be a car with a local trust server built-in that verifies a wireless digital certificate. The client may be a desktop computer, cell phone, ATM machine, credit card verifiers, security servers, access control systems, smart card readers, or any other type of system.

[0099] FIG. 15 is a block diagram illustrating a trust server 214 that validates security credentials locally within an enterprise 212. More specifically, trust server 214 intercepts validation requests to external validation services and answers the validation requests locally. Trust server 214 includes a client service interface 224, a validation service 226, a directory 228, a bridge provider interface 230, and a policy enforcement service 232.

[0100] Client service interface 224 couples client services to trust server 214 to allow trust server 214 to intercept validation requests from client services and perform substantially instant validation. Client service interface 224 may couple client service software, such as the secure email client software described above, to trust server 214. Client interface 224 may be, for example, an application program interface (API).

[0101] Upon trust server 214 intercepting a validation request, validation service 226 begins the validation process. Validation process 226 may access a directory 228 to search for security credential information for the validation process.

Directory 228 may include, for example, validate dates of the digital certificate, the status of the digital certificate (i.e., active or revoked), XML-structured contact information for the client associated with the digital certificate, and any client security credentials information specific to a service. For example, for a purchasing service, client security credentials for the specific service may include an amount a client has the authority to commit the enterprise to in purchasing or contracting.

[0102] When validation process 226 finds the necessary information within directory 228, validation process 226 parses the security credential information and processes the security credential information in order to control the client service. If validation process 226 validates the security credentials, the client service may continue with the services provided.

[0103] When validation process does not find the necessary security credential information, trust server 214 communicates a query for the security credential information to a bridge service provider 216 via bridge provider interface 230. Bridge provider interface 230 may also provide a communication path by which bridge service providers 216 may query trust server 214 for security credential information. Bridge provider interface 230 may also be an application programmable interface (API).

[0104] Policy enforcement service 232 controls the sharing of security credential information with other enterprises via bridge service providers 216. For instance, policy enforcement service 232 may allow a first enterprise 212 with a first permission level to security credential information and may grant a second enterprise 212 with less permission than the first.

[0105] FIG. 16 is a block diagram illustrating a bridge service provider 216 that links trust servers 214 together to form a trust domain, such as trust domain 210 of FIG. 13. Bridge service provider 216 includes a trust server interface 234, a bridge provider interface 236, and a member directory 238.

[0106] Bridge service provider 216 receives queries from trust servers 214 via trust server interface 234. Bridge service provider 216 may access memory directory 238 in response to the query to obtain security credential information for the validation. Memory directory 238 may include, for example, a unique identifier, a

certificate number, and a reference for security credential information location for each of the members. The reference for security credential information may, for instance, be a lightweight directory access protocol (LDAP) directory. Bridge service provider 216 may relay security credential information obtained in response to the queries to trust servers 214 via trust server interface 234.

[0107] Bridge service provider 216 may also forward the queries to a trust server 214 of another enterprise and relay the responses to the querying trust server via trust server interface 234. Although a single trust service interface 234 is illustrated in the example of FIG. 16, bridge service provider 216 may include more than one trust service interface 234 in order to interface different security models of different enterprises 212.

[0108] Bridge service provider 216 may also forward the queries from trust servers 214 to another bridge service provider 216 via bridge provider interface 236. The information received from the other bridge service provider 216 may is relayed back to bridge service provider 216 via bridge provider interface 236 and then further relayed to the querying trust server 214 via trust server interface 234.

[0109] FIG. 17 is a flow diagram illustrating instant validation of security credential information locally within an enterprise 212. Trust server 214 intercepts a validation request from a client (242). The validation request may, for example, be intercepted in route to an external validation service.

[0110] Trust server 214 checks locally for the security credential information necessary to answer the validation request (244). Trust server 214 may, for example, be linked to or be a part of a certificate authority system within enterprise 212 and answer the validation request using a local certificate revocation list (CRL) or an online certificate status protocol (OCSP) responder. Alternatively, trust server 214 may be loaded with the security credential information in a directory, such as a cache, or other storage mechanism.

[0111] When trust server 214 does not have the necessary credential information, trust server 214 queries a bridge service provider 216 associated with trust server 214 (246, 248). Bridge service provider 216 determines whether a member directory has the necessary security credentials for the validation request (250). The directory may include, for example, a unique identifier, a certificate number,

and a reference for security credential information location for each member of bridge service provider 216. The reference for security credential information may, for instance, be a lightweight directory access protocol (LDAP) directory. Alternatively, bridge service provider 216 may answer the query on behalf of their clients by running local trust servers.

[0112] When bridge service provider 216 does not have the necessary security credential information, bridge service provider 216 queries a trust server 214 of the enterprise that may have the necessary security credential information (252). Alternatively, another bridge service provider 216 may be queried in hopes of trying to obtain the necessary security credential information.

[0113] When the bridge service provider 216 obtains the security credential information from the member directory or from the trust server of the other enterprise, bridge service provider 216 relays the security credential information back to the trust server 214 that intercepted the validation request (254). Trust server 214 parses the security credential information, processes the security credential information, and answers the validation request in accordance with the security credential information (256). When trust server 214 grants the validation request, the client service that sent the validation request provides the client service.

[0114] Various embodiments of the invention have been described. Nevertheless, it is understood that various modification can be made without departing from the spirit and scope of the invention. These and other embodiments are within the scope of the following claims.

CLAIMS:

1. A system comprising:

a client service executing within an enterprise; and

a trust server to receive validation requests from the client service and perform security credential validation within the enterprise.

2. The system of claim 1, wherein the trust server intercepts validation requests intended for external validation services.

3. The system of claim 1, wherein the trust server obtains security credential information for use in the security credential validation from within the enterprise.

4. The system of claim 3, wherein the trust server obtains the security credential information from one of a local certificate revocation list (CRL), an online certificate status protocol (OCSP) response, and a cache.

5. The system of claim 1, further comprising a bridge service provider to link the trust server with trust servers of other enterprises.

6. The system of claim 5, wherein the trust server queries the bridge service provider to obtain security credential information for use in validation within the enterprise.

7. The system of claim 6, wherein the trust server queries the bridge service provider when the security credential information is not found within the enterprise.

8. The system of claim 5, wherein the bridge service provider maintains a member directory and accesses the member directory to obtain the security credential information.

9. The system of claim 8, wherein the member directory includes a unique identifier, a certificate number, and a reference for a location of security credential information for each of the members.

10. The system of claim 9, wherein the reference for the location of security credential information includes a lightweight directory access protocol (LDAP) directory.

11. The system of claim 5, wherein the bridge service provider queries one of the trust servers of another enterprise for the security credential information.

12. The system of claim 11, wherein the enterprise of the querying trust server and the enterprise of the other trust server operate in different trust environments.

13. The system of claim 12, wherein the different trust environments include Public Key Infrastructure (PKI), Pretty Good Privacy (PGP), and Kerberos.

14. The system of claim 5, wherein the bridge service provider queries another bridge service provider for the security credential information.

15. The system of claim 5, wherein the bridge service provider relays the security credential information to the trust server that initiated the query.

16. The system of claim 1, wherein the trust server validates certificates from various Certification Authorities.

17. The system of claim 1, wherein the trust server logs validations to provide an audit trail.

18. The system of claim 1, wherein the client service includes a secure electronic mail (email) service, securely exchanging information, such as

electronic mail, electronic file sharing, network storage, secure web folders, secure web access, and the like.

19. A method comprising:

receiving a validation request from a client service within an enterprise; and

performing security credential validation within the enterprise using a trust server.

20. The method of claim 19, wherein receiving the validation request from the client service includes intercepting a validation request from the client service to an external validation services.

21. The method of claim 19, further comprising obtaining security credential information for use in performing security credential validation.

22. The method of claim 20, wherein obtaining security credential information for use in performing security credential validation includes obtaining security credential information within the enterprise.

23. The method of claim 22, wherein obtaining security credential information within the enterprise includes obtaining security credential information from one of a local certificate revocation list (CRL), an online certificate status protocol (OCSP) response, and a cache.

24. The method of claim 23, further comprising coupling the trust server to a bridge service provider to link the trust server with trust servers of other enterprises.

25. The method of claim 24, further comprising querying the bridge service provider to obtain security credential information for performing security credential validation.

26. The method of claim 24, wherein the bridge service provider obtains security credential information from a member directory.

27. The method of claim 26, wherein the member directory includes a unique identifier, a certificate number, and a reference for a location of security credential information for each of the members.

28. The method of claim 24, further comprising forwarding the query to one of the trust servers of another enterprise to obtain security credential information

29. The method of claim 28, wherein the enterprise of the querying trust server and the enterprise of the other trust server operate in different trust environments.

30. The method of claim 29, wherein the different trust environments include Pretty Good Privacy (PGP) and Kerberos.

31. The method of claim 24, further comprising forwarding the query to another bridge service provider to obtain credential information.

32. The method of claim 24, further comprising relaying the security credential information to the trust server that initiated the query.

33. The method of claim 19, further comprising:
parsing the security credential information; and
processing the parsed security credential information to answer the validation request.

34. The method of claim 19, further comprising logging validation requests to provide an audit trail.

35. The method of claim 19, wherein performing security credential validation includes performing security credential validation for certificates from various Certification Authorities.

36. The method of claim 19, wherein the trust server is associated with the client service.

37. The method of claim 19, wherein the client service includes a secure electronic mail (email) service, securely exchanging information, such as electronic mail, electronic file sharing, network storage, secure web folders, secure web access, and the like.

38. The method of claim 19, wherein the client service executes on a network device.

39. A system comprising:

a server having a directory of members of a network community, wherein the directory stores data defining digital identities of the members for securely exchanging information with the members; and

a software application executing on a network device coupled to the server for exchanging information between the members, wherein the software application accesses the directory and exchanges the information in accordance with the digital identities of the members.

40. The system of claim 39, wherein the directory stores member objects that define the digital identities as attributes of the members.

41. The system of claim 40, wherein the member objects conform to the Lightweight Directory Access Protocol (LDAP).

42. The system of claim 39, wherein the digital identities includes at least one of a digital certificate and a digital encryption key.

43. The system of claim 39, further comprising a directory management module to update the digital identities of the members in response to input from a registration agent.

44. The system of claim 43, wherein the directory management module updates the data to define new member in response to input from the registration authority, and associates a digital certificate with the digital identity of the new member.

45. The system of claim 43, wherein the directory management module requests the digital certificate from a certificate authority, and installs the digital certificate within the directory for access by the software application.

46. The system of claim 45, wherein the server stores policy information, and the directory management module controls the membership within the directory in accordance with the policy information.

47. The system of claim 46, wherein the policy information defines policies for the addition and removal of members to and from the community directory, and any digital identities required for the members of the community.

48. The system of claim 39, wherein the software application comprises one of a an electronic mail service, electronic file sharing service, network storage service, secure web folders, web-based email application, secure web access, a packet routing application, and a firewall application.

49. The system of claim 39, wherein the software application receives a request to exchange information from an originating member to a receiving member, and accesses the directory to retrieve the digital identity for the receiving member.

50. The system of claim 49, wherein the directory automatically validates the digital identity of the receiving member, and returns the digital identity of the

receiving member to the software application, wherein the software application applies formulates and sends a secure electronic communication to the member based on the received digital identity.

51. The system of claim 50, wherein the directory verifies that the digital identity has not been revoked, and that the recipient member is a current member of community.

52. A system comprising

a community directory of members of a network community, wherein the members are associated with a plurality of enterprises;

a plurality of enterprise directories linked to the community directory, wherein the enterprise directories stored data defining digital identities for subsets of the members associated with the enterprises; and

a software application operating within a first one of the enterprises for exchanging information between the members of the community, wherein the software application accesses the enterprise directory associated with the first enterprise to securely exchange the information in accordance with the digital identities of the members.

53. The system of claim 52, wherein the software application receives a request to exchange information from an originating member within one of the enterprises to a receiving member within a different one of the enterprise, and accesses the first enterprise directory to retrieve the digital identity for the receiving member.

54. The system of claim 53, wherein the first enterprise directory validates the digital identity of the receiving member, and returns the digital identity of the receiving member to the service.

55. The system of claim 54, wherein the first enterprise directory queries the community directory for the digital identity of the receiving member.

56. The system of claim 55, wherein the community directory queries a second enterprise directory of an enterprise associated with the receiving member to retrieve the digital identity of the receiving member.

57. The system of claim 56, wherein the enterprise directories replicate all or portions of the data stored within enterprise directories to the community directory.

58. The system of claim 52, wherein the enterprise directories stores member objects that define the digital identities as attributes of the members.

59. The system of claim 58, wherein the member objects conform to the Lightweight Directory Access Protocol (LDAP).

60. The system of claim 52, wherein the digital identifies includes at least one of a digital certificate and a digital encryption key.

61. A method comprising:

receiving a request for exchanging information with a member of a network community;

accessing a directory to retrieve a digital identity for the member;

applying the digital identity to the information to produce a secure communication; and

sending the secure communication to the member.

62. The method of claim 61, wherein accessing a directory comprises accessing a community directory storing digital identities for all of the members of the community;

63. The method of claim 61, wherein accessing a directory comprises accessing an enterprise directory that stores digital identities for members of one of a plurality of enterprises associated with the community.

64. The method of claim 63, wherein the enterprise directory is linked to a community directory, the method further comprising accessing the directory community when the enterprise community does not include the digital identity for the member.

65. The method of claim 61, wherein accessing a directory comprises accessesing a directory of member objects that define digital identities as attributes of the members.

66. The method of claim 65, wherein accessing the member objects comprises accessing the member objects in accordance with the Lightweight Directory Access Protocol (LDAP).

67. The method of claim 61, wherein the digital identifies includes at least one of a digital certificate and a digital encryption key.

68. The method of claim 61, further comprising:

presenting an interface to receive input from a registration agent authorized to modify the directory; and

updating the digital identify of the member in response to the input.

69. The method of claim 68, further comprising:

defining a new member within the directory in response to input from the registration authority; and

associating a digital certificate with the digital identity of the new member.

70. The method of claim 69, further comprising:

requesting the digital certificate from a certificate authority in response to the input; and

automatically installing the digital certificate within the directory.

71. The method of claim 70, further comprising:
receiving policy information from the registration agent; and
controlling the membership within the directory in accordance with the policy information.

72. The method of claim 71, wherein the policy information defines policies for the addition and removal of members to and from the community directory, and any digital identities required for the members of the community.

73. The method of claim 61, wherein the secure communication comprises one of a an electronic mail and an electronic file.

74. The method of claim 61, wherein receiving a request comprises receiving a request to exchange information from an originating member to a receiving member, and accesses the directory comprises accessing the directory to retrieve the digital identity for the receiving member.

75. The method of claim 74, the digital identity includes at least one of a digital certificate and a digital encryption key.

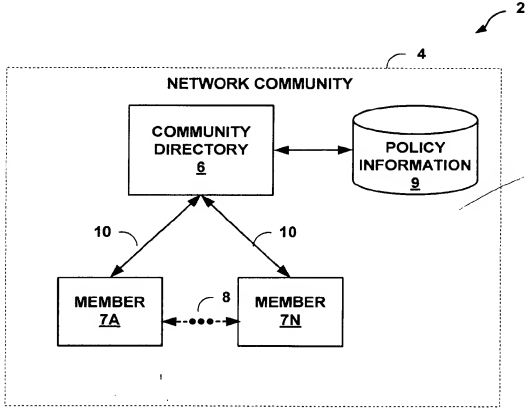

2
4
NETWORK COMMUNITY
COMMUNITY DIRECTORY 6
POLICY INFORMATION 9
10
10
8
MEMBER 7A
MEMBER 7N

FIG. 1

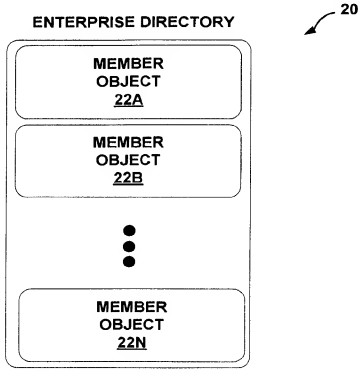

ENTERPRISE DIRECTORY
20
MEMBER OBJECT 22A
MEMBER OBJECT 22B
MEMBER OBJECT 22N

FIG. 2

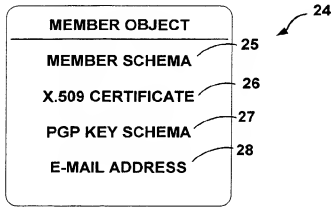

MEMBER OBJECT
24
MEMBER SCHEMA
25
X.509 CERTIFICATE
26
PGP KEY SCHEMA
27
E-MAIL ADDRESS
28

FIG. 3

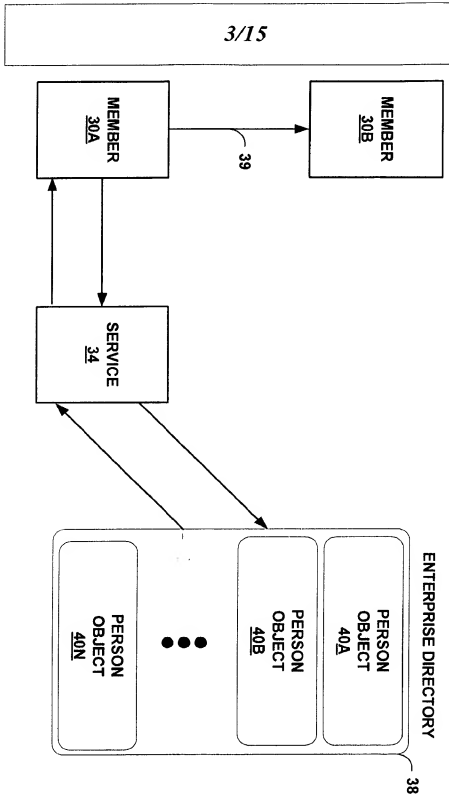

MEMBER
30B
MEMBER
30A
39
SERVICE
34
ENTERPRISE DIRECTORY
PERSON
OBJECT
40A
PERSON
OBJECT
40B
PERSON
OBJECT
40N
38

FIG. 4

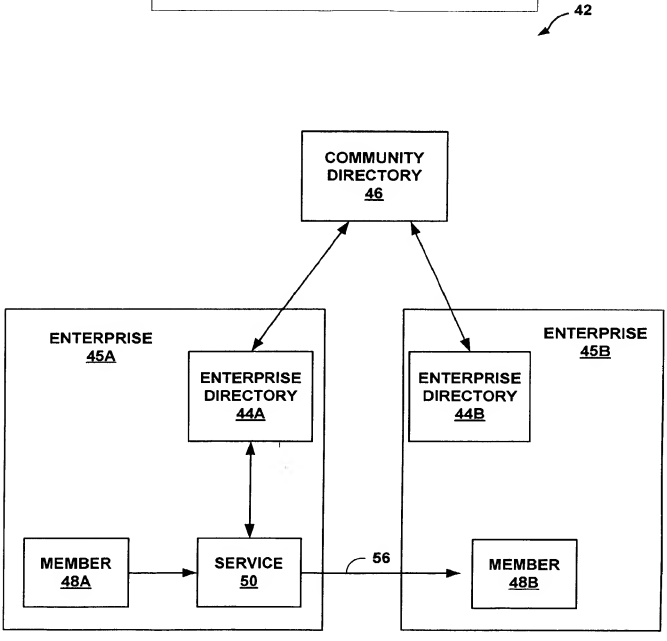

42
COMMUNITY DIRECTORY 46
ENTERPRISE 45A
ENTERPRISE DIRECTORY 44A
ENTERPRISE DIRECTORY 44B
ENTERPRISE 45B
MEMBER 48A
SERVICE 50
56
MEMBER 48B

FIG. 5

REGISTRATION AGENT 60
DIRECTORY MANAGEMENT MODULE 64
COMMUNITY DIRECTORY 62
POLICY INFORMATION 78
ENTERPRISE 74
REGISTRATION AGENT 66
DIRECTORY MANAGEMENT MODULE 68
ENTERPRISE DIRECTORY 72
MEMBERS 70
SERVICE 80

FIG. 6

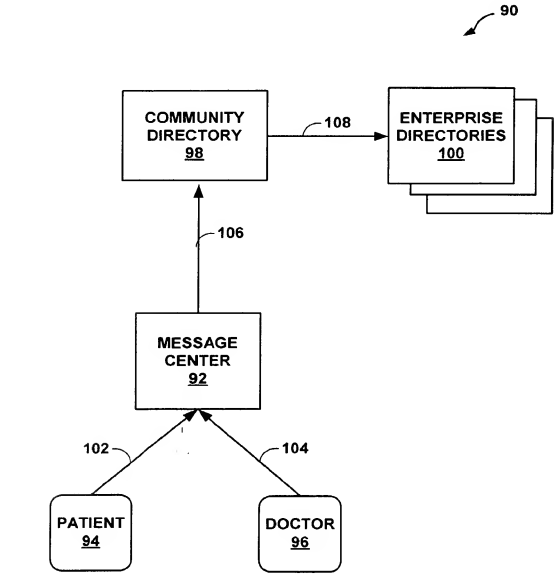

90
COMMUNITY DIRECTORY 98
108
ENTERPRISE DIRECTORIES 100
106
MESSAGE CENTER 92
102
104
PATIENT 94
DOCTOR 96

FIG. 7

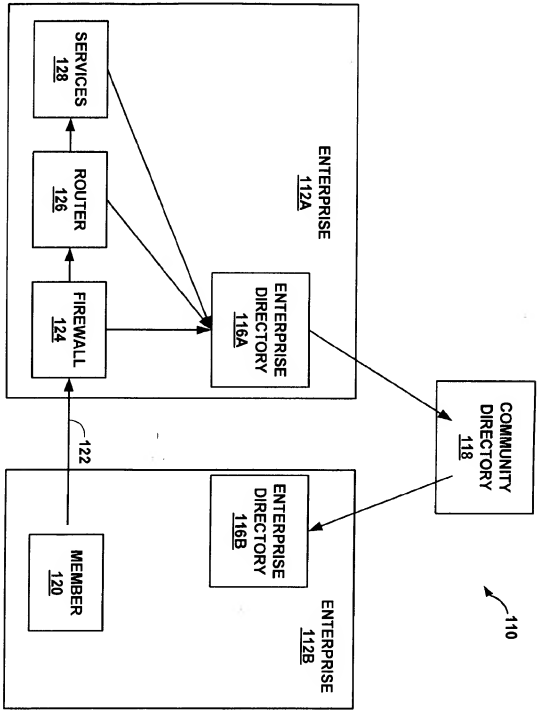

COMMUNITY DIRECTORY 118
110
ENTERPRISE 112A
ENTERPRISE DIRECTORY 116A
SERVICES 128
ROUTER 126
FIREWALL 124
122
ENTERPRISE 112B
ENTERPRISE DIRECTORY 116B
MEMBER 120

FIG. 8

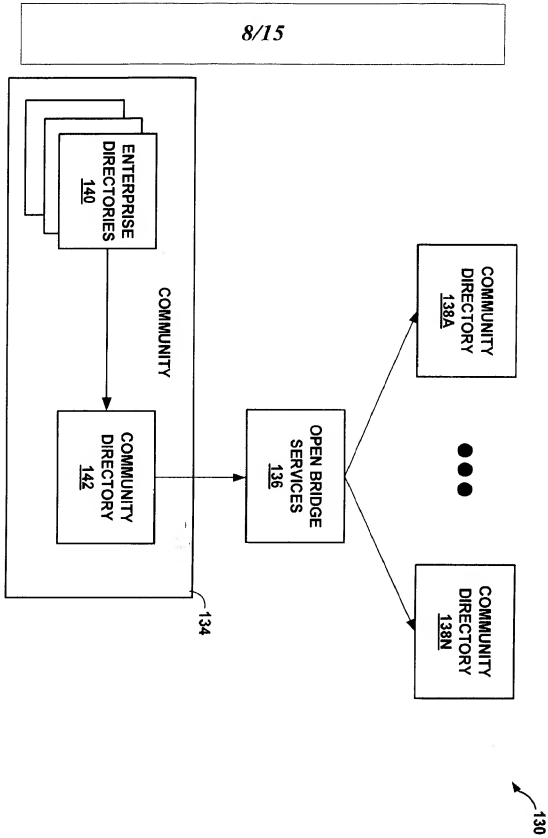

COMMUNITY DIRECTORY 138A
COMMUNITY DIRECTORY 138N
OPEN BRIDGE SERVICES 136
ENTERPRISE DIRECTORIES 140
COMMUNITY
COMMUNITY DIRECTORY 142
134
130

FIG. 9

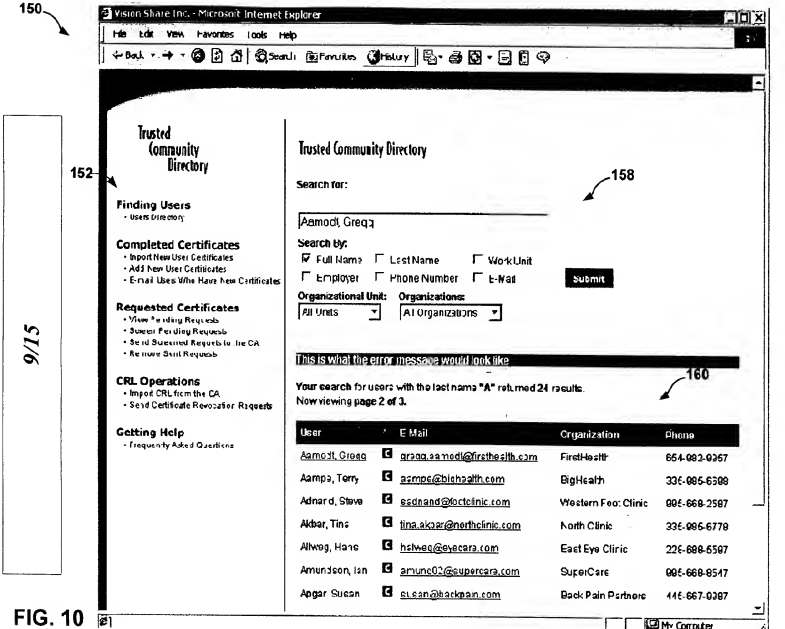

150
Vision Share Inc. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
152
Trusted Community Directory
Finding Users
• Users Directory
Completed Certificates
• Import New User Certificates
• Add New User Certificates
• E-mail Users Who Have New Certificates
Requested Certificates
• View Pending Requests
• Screen Pending Requests
• Send Screened Requests to the CA
• Remove Sent Requests
CRL Operations
• Import CRL from the CA
• Send Certificate Revocation Requests
Getting Help
• Frequently Asked Questions
Trusted Community Directory
158
Search for:
Aamodt, Gregg
Search by:
Full Name
Last Name
Work Unit
Employer
Phone Number
E-Mail
Submit
Organizational Unit:
All Units
Organizations:
All Organizations
This is what the error message would look like
160
Your search for users with the last name "A" returned 24 results.
Now viewing page 2 of 3.
User
E Mail
Organization
Phone
Aamodt, Gregg
greggaamodt@firsthealth.com
FirstHealth
654-982-0367
Aampa, Terry
aampa@bighealth.com
BigHealth
336-986-6308
Adnard, Steve
esdnand@doctelnic.com
Western Fed. Clinic
986-668-2587
Akbar, Tina
tina.akbar@northclinic.com
North Clinic
336-986-6778
Allweg, Hans
hsllweg@eyecare.com
East Eye Clinic
226-688-6587
Amundson, Ian
amunc02@supercare.com
SuperCare
986-668-8547
Apgar Susan
susan@backpain.com
Back Pain Partners
446-667-0387
My Computer

FIG. 10

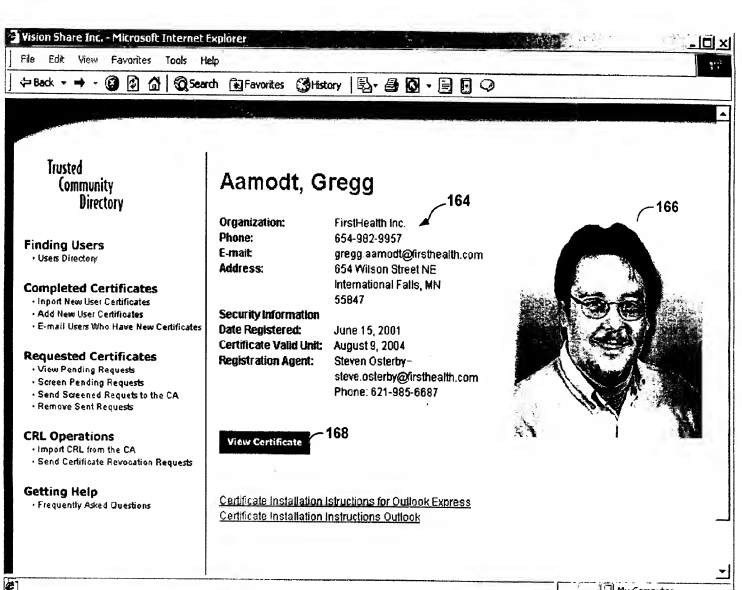

162
Vision Share Inc. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Trusted Community Directory
Finding Users
• Users Directory
Completed Certificates
• Import New User Certificates
• Add New User Certificates
• E-mail Users Who Have New Certificates
Requested Certificates
• View Pending Requests
• Screen Pending Requests
• Send Screened Requets to the CA
• Remove Sent Requests
CRL Operations
• Import CRL from the CA
• Send Certificate Revocation Requests
Getting Help
• Frequently Asked Questions
Aamodt, Gregg
164
166
Organization: FirstHealth Inc.
Phone: 654-982-9957
E-mail: gregg.aamodt@firsthealth.com
Address: 654 Wilson Street NE
International Falls, MN
55847
Security Information
Date Registered: June 15, 2001
Certificate Valid Until: August 9, 2004
Registration Agent: Steven Osterby~
steve.osterby@firsthealth.com
Phone: 621-985-6687
View Certificate
168
Certificate Installation Istructions for Outlook Express
Certificate Installation Instructions Outlook
My Computer

FIG. 11

170
Customer Community Directory - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Manage Customers
Search
Add Customer
Server Status
Home
Dashboard
Reporting Logs
View Certificate
Back
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 75 (0x4b)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=Minnesota, L=St Paul, O=VisionShare INC, OU=VisionShare,
Validity
Not Before: Aug 2 22:06:30 2001 GMT
Not After : Aug 20 22:06:30 2003 GMT
Subject: C=US, ST=Minnesota, L=Minneapolis, O=Golden Plate Glass, OU=Filling,
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c1:8b:42:6d:4d:e5:23:7e:06:d6:e0:ff:de:
35:d0:6b:97:c4:1f:c6:c1:d1:bd:bf:64:e4:2d:b1:
a7:5b:31:2c:c4:40:9e:26:6d:94:ca:50:7e:5a:1c:
82:49:6a:9b:b4:af:55:fa:e5:69:9b:d8:c7:17:df:
c4:64:33:f9:1c:e4:29:c3:c4:d0:03:19:50:4f:cc:
cc:10:39:bb:e5:9f:35:47:d7:6b:9d:3d:
11:e9:7b:bd:fc:d1:36:6a:ba:05:b8:16:45:38:bf:
fc:a3:6a:9d:22:ef:ed:93:b3:60:2a:b0:6c:ec:2c:
ac:1d:4d:29:e2:1c:ad:a3:a3
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
Done
Internet

FIG. 12

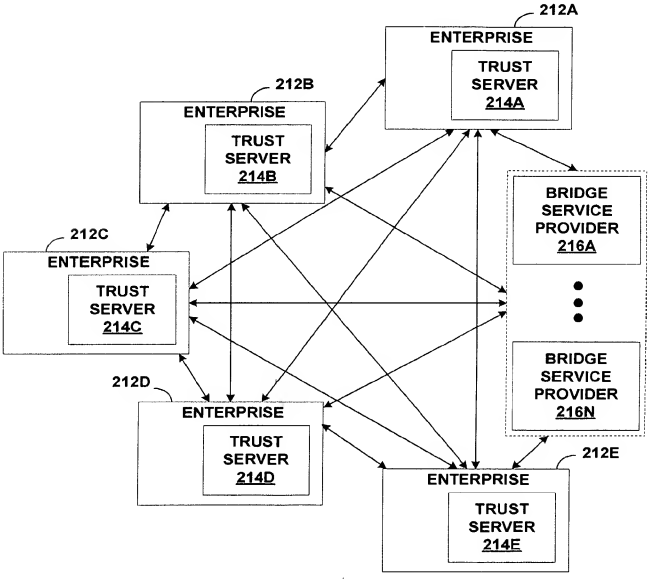

210
212A
ENTERPRISE
TRUST SERVER 214A
212B
ENTERPRISE
TRUST SERVER 214B
212C
ENTERPRISE
TRUST SERVER 214C
212D
ENTERPRISE
TRUST SERVER 214D
212E
ENTERPRISE
TRUST SERVER 214E
BRIDGE SERVICE PROVIDER 216A
BRIDGE SERVICE PROVIDER 216N

FIG. 13

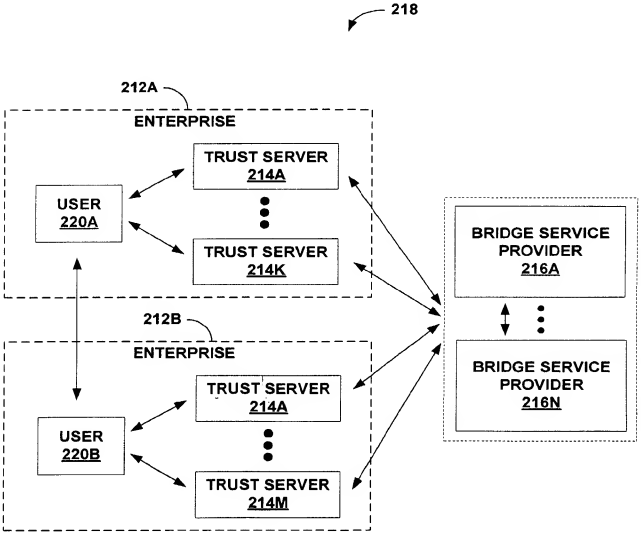

218
212A
ENTERPRISE
TRUST SERVER
214A
USER
220A
TRUST SERVER
214K
212B
ENTERPRISE
TRUST SERVER
214A
USER
220B
TRUST SERVER
214M
BRIDGE SERVICE
PROVIDER
216A
BRIDGE SERVICE
PROVIDER
216N

FIG. 14

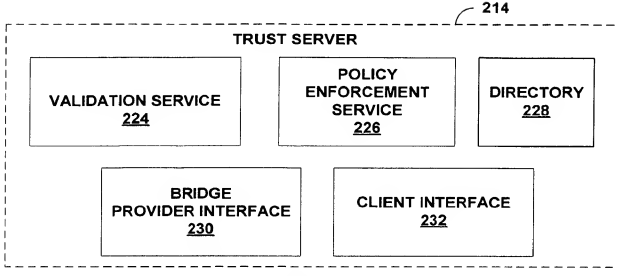

214
TRUST SERVER
VALIDATION SERVICE
224
POLICY
ENFORCEMENT
SERVICE
226
DIRECTORY
228
BRIDGE
PROVIDER INTERFACE
230
CLIENT INTERFACE
232

FIG. 15

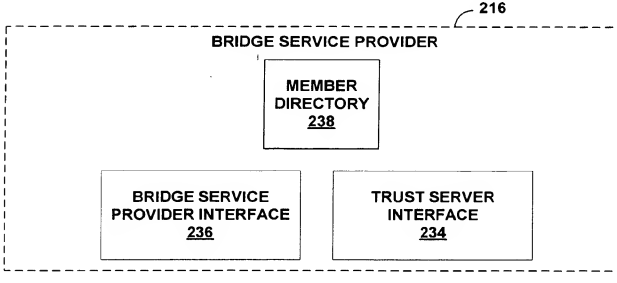

216
BRIDGE SERVICE PROVIDER
MEMBER
DIRECTORY
238
BRIDGE SERVICE
PROVIDER INTERFACE
236
TRUST SERVER
INTERFACE
234

FIG. 16

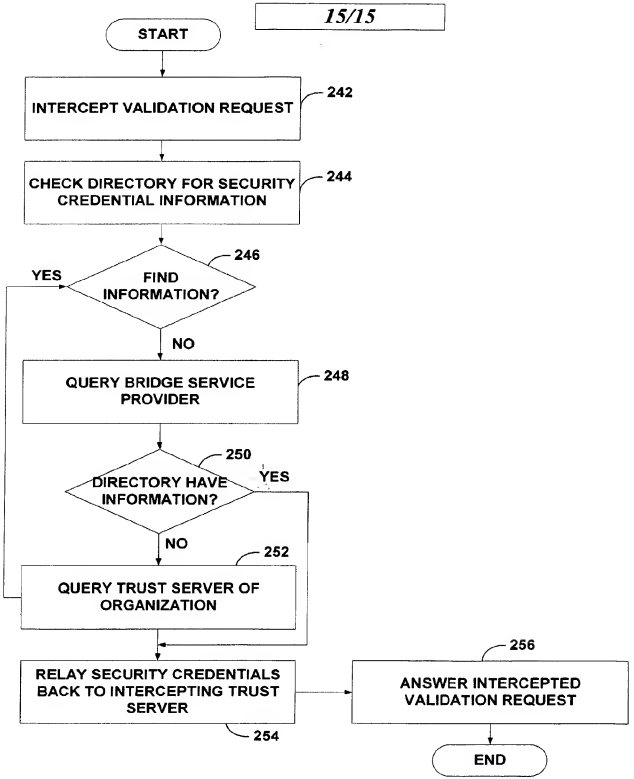

START
INTERCEPT VALIDATION REQUEST
242
CHECK DIRECTORY FOR SECURITY CREDENTIAL INFORMATION
244
FIND INFORMATION?
246
YES
NO
QUERY BRIDGE SERVICE PROVIDER
248
DIRECTORY HAVE INFORMATION?
250
YES
NO
QUERY TRUST SERVER OF ORGANIZATION
252
RELAY SECURITY CREDENTIALS BACK TO INTERCEPTING TRUST SERVER
254
ANSWER INTERCEPTED VALIDATION REQUEST
256
END

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/38231

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/16

US CL : 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/155,168,170,176,189201; 709/203,23;380/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,067,623 A (BLAKLEY, III et al.) 23 May 2000 (23.05.2000), abstract, Fig.2 , Col. 3, lines 9-40, col. 5, line 32 through col. 6, line 11.	1, 19,39,52 ---------- 2-18,20-38,40-51, 53-75
Y, P	US 2002/0087670 A1 (EPSTEIN et al.) 04 July 2002 (04.07.2002), abstract, page 2, paragraphs 17-21, Fig. 2, paragraph 27, claim 1	2-18
Y,P	US 2002/0144111 A1 (AULL) 03 October 2002 (03.10.2002), the entire document.	2-18, 20-38, 40-51, 53-75
Y,P	US 2002/009157 A1 (CUOMO et al.) 11 July 2002 (11.07.2002), the entire document.	2-18, 20-38,40-51, 53-75
X	US 6,215,872 B1 (VAN OORSCHOT) 10 April 2001 (10.04.2001), the entire document.	1,19,39,52

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 2003 (20.02.2003)	01 APR 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer Taghi T. Arani
Facsimile No. (703)305-3230	Telephone No. (703) 305-4274

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US02/38231

Continuation of B. FIELDS SEARCHED Item 3:
WEST, ProQuest, Dialog. Search Terms: trust adj association same community adj member$4, directory adj centric and trust adj server$2, community adj chat adj room or trusted adj community